MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Miden

On June 15, 2026, Crypto Task Force Staff met with representatives from Miden.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Miden representatives provided the attached document, which was discussed during the meeting.

Miden Proposed SEC Crypto Task Force Meeting Request

Proposed Attendees

- Azeem Khan, Co-Founder, Miden
- Irakliy Khaburzaniya, Co-Founder, Miden

Detailed Meeting Agenda and Discussion Topics

Miden is a zero-knowledge blockchain infrastructure platform focused on compliant privacy, client-side proving, and user-controlled data architectures. The purpose of this meeting is to provide the SEC Crypto Task Force with an overview of several emerging technical design approaches that we believe may become increasingly relevant to digital asset infrastructure, institutional adoption, cybersecurity, and future compliance frameworks.

The meeting would focus on the following topics:

1. Introduction to Miden and Current Development Status

We would provide a brief overview of Miden's architecture, current stage of development, and long-term focus on privacy-preserving blockchain infrastructure. This would include discussion of Miden's client-side proving architecture, localized data storage, assisted self-custody model, and selective disclosure capabilities intended to support both user privacy and regulatory compliance requirements.

We would also discuss our broader philosophy around building blockchain infrastructure intended for long-term institutional and enterprise participation rather than short-term speculative activity.

As part of this approach, we have intentionally chosen not to launch a native token at the current stage of network development. We believe it is important to first mature the underlying technology, operational architecture, and compliance frameworks of the network before introducing additional market structure complexity.

We would also welcome broader discussion around how evolving digital asset market structure proposals and regulatory developments in the United States may shape long-term infrastructure design decisions for blockchain networks.

2. Client-Side Proving and Localized Data Storage

We would discuss Miden's client-side proving architecture, where cryptographic proofs are generated locally rather than requiring sensitive user data to be broadly distributed across network participants. We believe this design approach may have implications for user privacy, cybersecurity, institutional adoption, and data handling requirements in regulated environments.

The discussion would also explore how increased off-chain computation may reduce unnecessary public exposure of transaction and account data while still preserving verifiability and auditability.

Additionally, we believe privacy-preserving infrastructure should increasingly be viewed through the lens of cybersecurity and operational risk reduction. Publicly exposing wallets, balances, treasury movements, and transaction histories may create unnecessary security vulnerabilities for institutions, businesses, and users operating on blockchain networks.

3. Assisted Self-Custody and the Guardian Model

We would demonstrate Miden's "Guardian" framework, which is designed to support assisted self-custody, configurable compliance requirements, and selective disclosure capabilities without requiring full custodial control by intermediaries.

This discussion would focus on how blockchain systems may support recoverability, compliance controls, and real-time monitoring capabilities while still preserving user ownership and exit rights. We believe these topics may become increasingly important as digital asset infrastructure evolves toward institutional participation.

We would also discuss how Guardian operators may support varying compliance environments while operating on shared blockchain infrastructure.

4. Selective Disclosure, Compliance, and Institutional Requirements

We would discuss broader questions around how privacy-preserving technologies may coexist with compliance obligations, including selective disclosure frameworks, auditability, and permissioned compliance environments operating on shared infrastructure.

The purpose of this section would not be to advocate for any specific regulatory outcome, but rather to provide technical context around how modern zero-knowledge systems may differ from earlier blockchain architectures that relied primarily on full public transparency.

We believe there may be opportunities for blockchain systems to support both regulatory visibility and user privacy simultaneously, depending on the architecture and operational design choices implemented.

5. Stablecoin-Denominated Fees and Alternative Network Models

We would also welcome discussion around our exploration of stablecoin-denominated transaction fees and whether alternative fee models may reduce friction and speculation associated with native token dependency in blockchain networks.

This section would focus on user experience, operational stability, and broader questions around how blockchain infrastructure may evolve in regulated financial environments.

6. Phased Network Decentralization and Operational Safety

We would also welcome discussion around the operational realities of launching new blockchain infrastructure responsibly. In particular, we believe there are important tradeoffs between immediate decentralization claims and the practical requirements of security, reliability, compliance readiness, and user protection during early network stages.

We would discuss our current approach to phased decentralization, including why certain operational components may initially remain more centralized during early deployment while the network matures and security assumptions are validated over time.

We believe greater industry clarity around responsible decentralization pathways may benefit both developers and regulators as blockchain infrastructure continues to evolve.

7. Architectural Tradeoffs Across Privacy and Institutional Blockchain Systems

As part of the discussion, we would also welcome the opportunity to discuss how different blockchain privacy and institutional infrastructure models approach questions around custody, compliance, governance, operator controls, user protections, and exit rights.

This would include broader discussion around varying architectural approaches currently emerging across the industry, including permissioned systems, zone-based compliance models, and privacy-preserving public blockchain infrastructure.

We would also welcome discussion around how different infrastructure models may create differing assumptions around counterparty risk, interoperability, jurisdictional concentration, and long-term network neutrality as digital asset infrastructure expands globally.

The purpose of this discussion would not be competitive positioning, but rather to help inform broader conversations around how different technical designs may create different regulatory, operational, cybersecurity, and user protection implications.